# News & Views

## How to Wage and Win the Long War

Gerry Yonas,
gyonas@sandia.gov

Now that we seem to have won the short war in Iraq, we need to get very serious about the tougher, long-term war against fundamentalist, militant, terrorist, murderous, evil-doers (FMTMEDs). To shorten the acronym, I will call this threat the FMs. The first thing we have to do is figure out who and where they are, what they plan to do to us, and how they plan to do it. We also need to know a lot more about their supporters and the—as yet—undecided population from which their supporters can draw recruits that could eventually become FMs. (We should remember that in Israeli/Palestinian math, if Israel defeats two out of ten terrorists then they are left with eight; in terrorist math, ten minus two equals twelve.) Winning will require that we get rid of the current FMs, discourage their supporters, and keep the undecided from becoming supporters.

To get rid of the FMs when we find them, we can destroy them and their tools, or put them away for a very long time, or maybe just compel them to quit the fight. To discourage supporters, who provide critical connections and resources, we need to create a sense of uncertainty, or even dread, about the FMs. But first, we need to destroy their admiration of, and trust in, the FMs. Such organizations as the FBI and law enforcement have used various techniques to create such divisions in the ranks of organized radical and criminal groups, and those methods might work here.

The most difficult issue in the long war, however, is how to dissuade the undecided, who ultimately will make the difference between our victory or defeat. Not only are there many, many more undecided, but many of them already lean toward becoming supporters because they really don't like our policies. There are also undecided who tend to dislike the FMs, but could be turned against us by such factors as fundamental disagreement with our ideology and methods, frustration with real or perceived personal losses, lack of patience with the long-term war, or lack of faith in our willingness to stay the course. In the long run, the real battleground will be over the hearts and minds of those in the middle of the spectrum of ideas, and we need not just a strategy but an actual program to deal with them.

It is likely that the people in the middle ground will be found in developing countries, and they will tend to be young—possibly very young. For instance, the
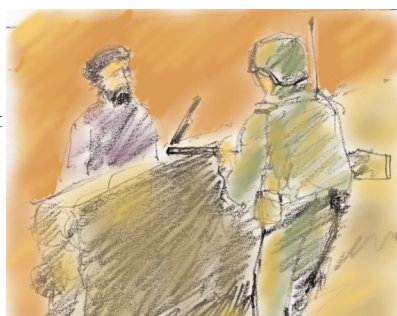


### Inside this issue

> **"For instance, the median age in many Arab countries is between 16 and 19, and many of these people are very unhappy, frustrated, and ready for a fight."**

median age in many Arab countries is between 16 and 19, and many of these people are very unhappy, frustrated, and ready for a fight. This is to be contrasted with developed countries that have median ages from 35 to 40, are growing older rapidly, and are already becoming weary of conflict and longing for stability and the status quo. According to our census bureau, in 2050 the median age in Germany and Japan will be 50. Their governments will be desperately trying to cope with the economic burden of the social contracts created a century before. They will be less and less willing to engage in any conflicts with other countries, especially those that do not pose an immediate threat to them. We should not look to them for much help in this war.

The dominant socio-economic issues in developing countries, particularly in the Arab world, are lack of education and dismal job opportunities for the increasing youth population. These young people are tending to concentrate in mega cities that will become the breeding grounds of future FMs. One suggested strategy to influence the undecided in developing countries is to enhance their economic status, education, and health in ways that enhance hope and self-esteem while limiting their resentment of those who are trying to help them.

Of course this "high road" approach might not work. Corrupt government, lack of property rights, or even minimal fairness in providing rewards for hard work and creativity, could divert contributed resources in ways that would just further empower and enrich the undeserving few while restricting the opportunities of the many. Another approach would be to take the "low road" where we could work to make life even more hopeless and miserable for the population—for instance, with economic sanctions—in hopes that they will throw off their corrupt rulers but not blame us for their misfortune or turn to more radical forms of governance. Recent history tells me that that this "low road" approach is unlikely to work.

As the next article explains, the "high road" is likely to be a long one, with an uncertain outcome, but it may be our best chance for winning the war. This will be a cooperative venture between us and the undecided to not only solve immediate problems, but also to create a shared vision of freedom, hope and prosperity for the future. ■

## Some Things to Know About Who's on the Internet

*Things are changing on the Internet faster than you can say, "Here comes India." It pays to keep up on who's out there. Here are a few trends.*

The number of baby boomers and seniors online grew by 18.4 percent last year, making them the fastest growing Internet population, according to Media Metrix. *According to Jupiter Research, this number will reach 16.3 million by the year 2007.*

Asian-American men spend 50% more time on the Internet than other multicultural groups. *However, Latino and Hispanic Americans represent the fastest-growing online ethnic group, according to new data from Nielsen//NetRatings.*

Online language populations on the Internet are as follows: English, 36.5%; Chinese, 10.9%; Japanese, 9.7%; Spanish, 7.2%, German, 6.7%, Korean, 4.5%, Italian, 3.8%; French, 3.5%; Portuguese, 3%; Russian, 2.9% and Dutch, 2%. (Source: Global Reach)

India could be second only to China in terms of Internet usage by 2004, according to a report by Credit Lyonnais Securities Asia.

According to Jupiter, online buyers over the age of 50 will account for almost 1/4 of all online retail spending by 2007.

95% of older online users (55+) say that email is their favorite activity, and 57% often send or receive egreetings and online postcards.

# Why Mexico Is Easy and Iraq Hard

Gary J. Jones,
gjjones@sandia.gov

Economic growth and middle class development are critical to the establishment of democratic governments and open societies. There have been numerous studies that have looked at the requirements and obstacles to middle class formation throughout the world. Authors, often focusing on requirements and obstacles defined by their theoretical interests, have identified a broad range of "key" issues. The problem is that all these authors are probably correct—each taking a different view of the development "elephant" and describing that view in detail. The challenge is to try to gain an appreciation of the complete set of requirements and obstacles, capturing all of these points of view.

One way to begin is to look at the United Nations Development Program's (UNDP) *Human Development* reports and their discussion of critical issues. If these issues are examined in detail they offer a broad view of the requirements for, and the obstacles to, middle class formation and economic development in societies. The UNDP's *Human Development Index* and the more recent *Alternative Human Development Index* from the UNDP *Arab Human Development Report 2002* (AHDR) focus on six key factors:

1. Life expectancy at birth
2. Adult literacy rate and combined enrollment rate at the primary, secondary, and tertiary education levels
3. Freedom; civil and political liberties
4. Gender empowerment
5. Technology
6. Environment

## Life Expectancy

The life expectancy term in the *Alternative Human Development Index* represents broad concepts, including the access to health care, a healthy environment, and a minimum quality of life for all members of society. It is considered to be the most basic aspect of the development requirements. Without a reasonable life expectancy value and the related lifetime health aspects, the rest of the individual empowerment elements have significantly reduced importance to the population.

## Literacy and Education

The adult literacy rate and the combined enrollment rates reflect the availability of education to all members of society. However, this is not only an issue of knowledge availability, but also knowledge acquisition and utilization. Mexico has a history of supporting higher education, but historically these scientists were discouraged from applied research with industry and developing products, and encouraged instead to conduct basic research. The same philosophy is more extensive in many Arab countries. Related to this is whether the society "celebrates" higher education and new business and product development. Certainly cultures that celebrate educational and business success seem to be more economically successful. We have seen this with Chinese and Vietnamese immigrants to the U.S. and with the Jews over history. As a corollary, societies that do not celebrate these types of success are often not economically successful. The lack of personal entrepreneurism in Japan has been attributed to the fear of "losing face" by failing. Bernard Lewis attributes the decline of the Arab excellence in science and corresponding civilizational decline from the 17th century onward to the emergence of a culture that did not celebrate understanding and progress and denigrated communication with "infidel" societies.

## Freedom and Liberties

The freedom factor focuses on personal freedom, economic freedom, access to capital, and the rule of law. It emphasizes the enhancement of human capabilities, reflecting the ability of people to achieve what they value. The AHDR identified five specific types of freedoms that need to be present for development:

1. POLITICAL FREEDOM: having a voice in the government and government being scrutinized about its role and actions.

2. ECONOMIC FACILITIES: the protection of individual assets, confidence that

> "Bernard Lewis attributes the decline of Arab excellence in science and the corresponding civilizational decline from the 17th century onward to the emergence of a culture that did not celebrate understanding and progress and denigrated communication with 'infidel' societies."

> "In locations with significant discrimination, the inequality of women often results in higher illiteracy rates, increased infant mortality, and shorter life expectancy for **society as a whole**."

what is earned is safe from expropriation, a free market with work valued independent of the worker's group or sex, and the ability to access capital for the development of small and medium sized enterprises.

3. SOCIETAL OPPORTUNITIES: the accessibility of all members of society to education and health care, employment, and protection, and equal pay for equal work or equal product.

4. TRANSPARENCY GUARANTEES: safeguarded social interactions between individuals, contracts in society.

5. PROTECTIVE SECURITY: social safety nets and the provision for the common good.

Much of the concept of the "rule of law" related to individual dealings ranging from contracts and equity to equality and self-determination are contained in this broad freedom concept. Achieving this freedom places explicit requirements on a country's institutions. One of the most important and least understood institutions is the development and support of property rights for all segments of society. Hernando De Soto, in his book, *The Mystery of Capitalism*, states that the reason why many countries do not have the capital base to fund development is that they have not implemented the concept of personal property and lack the ability to use property to gain access

to capital. Conversely, this lack fosters corruption through bribes and payoffs to achieve a substitute "business-like" environment.

### Gender

Gender inequality is one of the most devastating forms of discrimination. Wherever it is present, in the developed or developing world, it impacts broad aspects of society. Obviously restricting half or more of the population from the ability to constructively contribute to a country's economy handicaps economic development. Conversely, in countries without restrictions on lending and property, women rapidly become a major force in community development. In locations with significant discrimination, the inequality of women often results in higher illiteracy rates, increased infant mortality, and shorter life expectancy for **society as a whole**.

### Technology

The technology measure recognizes that economies can no longer be based solely on natural resources, but rather they must be based on the development of human resources. This shift has changed the possibilities for many natural-resource-poor countries and taken away opportunities for many natural-resource-rich countries. The importance of the reliance on human versus natural resource development is expressly addressed in many studies. The World Bank's *World Development Report 2003* states that economies dominated by natural resources often lead

to high inequalities in income, wealth, and human capital. Landes, in discussing the oil rich Middle East countries is more direct:

*"…the huge oil windfall has been a monumental misfortune. It has intoxicated rulers, henchmen, and purveyors, who have slept on piles of money, wasted it on largely worthless projects, and managed to exceed their figuratively (but not literally) limitless resources. Even Saudi Arabia cannot balance its books. In the process these spoilers have infuriated the Muslim poor, who in turn have sought an outlet for rage and outrage in fundamentalist doctrine."*

The *World Development Report* states that today it is not enough to have a single source of economic development. True economic sustainability "…depends on creating a never-ending supply of new opportunities." Today this requires a vibrant in-country technology base.

### Environment

The environment measure recognizes that a country's environmental inaction can destroy its ability to raise food and cause desertification, can destroy forests and rivers in order to support resource extraction, or overfish or overgraze impacting economy supporting operations.

### Conclusion

In this discussion I emphasized the broad spectrum of challenges for a country to develop a sustained and stable economy. The developed countries have had the good fortune to address most of these challenges over their history.

Much of the developing world, as former colonies or fragments of failed regimes, has not had the benefits of time and growth. Even so, some countries are in a more advantageous position than others. Mexico has met or is attempting to meet all of the requirements in the list at the beginning of this article. The *Bi-National Sustainability Lab* focuses on helping them with some of the remaining concerns, such as helping establish a culture focusing on development, addressing entrepreneurial risk aversion by making success more likely, and providing the entrepreneur with an added sense of empowerment through access to product realization, and business and financing expertise.

Many of the poorer countries in the world have a much longer way to go. Countries with low literacy rates, low life expectancy, high infant mortality, and little in the way of secondary and tertiary education are missing basic requirements, much less worrying about the appreciation of high technology directions within the culture. These are the challenges facing not only Afghanistan and Pakistan, but also Egypt, Iraq, most of sub-Saharan Africa, and many others. Working with these countries means beginning by addressing the basic needs and moving on to the remainder of the requirements over one or more generations. While the path will be long for countries so far from achieving basic institutional needs, until progress is made we should not expect stable benevolent governments in these countries, much less democracies. ■

# Beyond Iraq

Curtis Johnson, cjohnso@sandia.gov

### New Doctrine

The decision for war in Iraq signals a potential shift in U.S. policy. Iraq is part of what *New York Times* columnist, Thomas Friedman, calls the "world of disorder," regions characterized by terrorism, crime, corruption, and autocratic, unstable, or irresponsible governments. The real Administration concern appears to be that weapons of mass destruction and the world of disorder shouldn't mix. If this is to be a new doctrine, the U.S. will soon have to deal with several threats that appear on a par with Iraq, including Pakistan, Syria and North Korea. These daunting challenges and continuing internal disagreement are likely what is restraining the Administration from setting a clear, new doctrine on WMD.

What the Administration has stated about its long-term goals is even more ambitious.

The U.S. strategy for the war on terrorism calls for the prevention of terrorism by supporting the worldwide spread of capitalism, democracy, and civil liberties. The hypothesis is that this Western trinity forms the foundation for stable, ordered societies where terrorism dies on the vine (as is apparently happening to the militia movement in the U.S.). In other words, the strategic goal is to transform the world of disorder into the world of order.

This is a noble and peculiarly American goal. We believe in these things, not just for ourselves but for all people. And it is a simple, sound strategy that will succeed if given time. While all of us find something to fear in the tyranny of the masses, the invisible (and unfeeling) hand of capitalism, and what others will do with their civil liberties, the western trinity is uniquely successful in enabling disparate peoples to live together prosperously with peaceful transitions in government. And though the trinity is an acquired taste, there is historical reason to believe that these concepts sell themselves, so much so that they are deeply feared and mistrusted by the world of disorder. And this is, of course, one reason other Arab governments are displeased to see the Hussein regime toppled.

### Recommendations

If it is to pursue this goal, how should the U.S. go about it?

As the nation and the world worry over U.S.

> "The hypothesis is that this Western trinity forms the foundation for stable, ordered societies where terror-ism dies on the vine (as is apparently happening to the militia movement in the U.S.)."

> ## Quote of the Day...
> "It is no use saying, 'We are doing our best.' You have got to succeed in doing what is necessary."
>
> --Sir Winston Churchill

hegemony, only two possibilities seem to be under discussion: UN-sanctioned activity or virtual unilateralism. The globalists contend that the U.S. cannot possibly succeed in the War on Terrorism or the rebuilding of Iraq without help. The unilateralists contend that nothing much can be accomplished through the UN. Both are right. And the dichotomy is hogwash.

1. The U.S. would be wise to make its intentions very clear. It should proclaim as doctrine both its new WMD stance and its strategy for the war on terrorism. In short, it should become as predictable as possible, since it has chosen not to be controllable. This predictability will increase its influence with friends and reduce the threat perceived by the rest.

2. If spreading the trinity is the end, the United Nations is not the means. The aspirations and rhetoric (and bylaws and charter) of the UN must be distinguished from the reality. It is not clear that the UN, as an organization, stands for anything beyond aid to the poor and disadvantaged and multilateralism as a means to prevent World War IV. And how could a body representing the governments of—let's just take the "I's"—Iceland, India, Indonesia, Iran, Iraq, Ireland, Israel, and Italy stand for much more than that? The "I's" (and their 25 cohort groups) are not going to champion the western trinity and make it happen. And the UN is not a world government so much as a world forum.

3. Nevertheless, there is wisdom in the contrary opinions of France, Germany, Russia and others. It will not be easy to expand the world of order while acting in a disorderly fashion, to bomb and reform at once. The Administration would be wise not only to hear out the opposition but to weigh their advice carefully.

4. The U.S. should pursue the goal of spreading the western trinity through a coalition of true believers working actively toward that end, even sacrificing their self-interest on occasion. This would be a multilateral organization that stands for something and backs it up. It should be a project team first, and only secondarily a political, military, or economic alliance. The motivation would not be altruism. It would be a global "neighborhood association" dedicated to clean streets, low crime, weekly garbage collection, and rising property values. Such a coalition could slowly become the governing body the UN was intended to be.

### Conclusion

The international alliances established in the wake of World War II have steadily

---

**Comments from Richard A. Clarke, former Chairman, President's Critical Infrastructure Protection Board, and former Special Advisor to the President for Cyber Space Security, from an interview published in *2003 CQ Homeland Security Inc.***

"...It may, because of the lopsided military victory, seem like the risks we ran by electing to conduct this war were negligible. In fact, the extent of the risks and costs are not yet known. The sentiment that President Mubarak of Egypt had in mind when he said the war has created "100 bin laden's" was largely correct. The war as seen on TV in Islamic countries has dangerously increased the level of frustration, anger, and hatred directed at the U.S. It has given radical Islamic terrorists another target, U.S. personnel in Iraq. The seeds of future terrorism have been sown."

"...Our greatest security issue is our lack of adequate penetration of potential terrorist groups. We could bankrupt the country trying to fix all the vulnerabilities, although we must address many of them. Where we get the best return for our dollar is by penetrating terrorist groups and then disrupting them, as we did in the plot to blow up the Lincoln Tunnel and the United Nations building in NY, and in the numerous failed attempts to attack the U.S. abroad. Key to such an approach is a strong intelligence capability, at home and abroad, cooperation among agencies, good use of information technology, and the development of real expertise. All of that can and must be done consistent with our values about civil liberties."

lost relevance, and there is reason to fear new alignments based on religion, civilization, or economics. The right realignment for the U.S. would be one based on the western trinity that is idealistic in its goals for the global community and pragmatic and enterprising in its means.

WW II started out as the dictatorships of Europe against the democracies, and Churchill and Roosevelt certainly played up their role as defenders of the free world. Now is the time for the activist free world to come together not in mutual defense, but as a neighborhood alliance with a noble cause. It would be a shame to let UN pressure and our own naive views of that institution dissuade us from this cause. ■

# The Najaf Checkpoint

*Peter Merkle,*
*pbmerkl@sandia.gov*

*I*n any situation where the use of lethal weapons is appropriate and legal, less-lethal and humanitarian weapons should be considered desirable alternatives. There are innumerable commentaries and analyses concerning nonlethal or less-lethal weaponry (LLW), for and against. The arguments against the development and use of at least some LLW ring exceedingly hollow, given the tragedies of civilian casualties in Operation Iraqi Freedom. I was amazed that

forward U.S. military units, fully expecting to transit and occupy civilian areas, were apparently not ready to use LLW and procedures at vehicle checkpoints. The Pentagon's Joint Nonlethal Weapons Directorate (JNLWD) has a wide assortment of tested gear: flash bang grenades, rubber bullets, and spike mats, to name a few.

Replay the scenario of the passenger van filled with women and children approaching a checkpoint in Najaf, Iraq, on March 31, 2003. Perhaps the driver was distracted, faced sun glare, or had poor eyesight, and did not perceive or misunderstood the signal to stop. Perhaps the warning shot was not audible inside the Toyota van filled with noisy children (an M16 bullet going by actually sounds like a sharp "crack" rather than a "boom"). The shots fired into the engine may have panicked or even wounded the driver, as screams filled the van from other passengers. In desperation, speeding toward the checkpoint was perhaps a reflex to try to get by danger, or get the soldiers to recognize that they were only women and children. The soldiers at the checkpoint carried out their mission properly, by all accounts. A suicide taxicab had already killed four soldiers, and standing orders were to treat all suspicious vehicles as potential bombs. The soldiers are to be admired for their restraint in going through the sequence of signaling and warning before opening fire

on the van. However justified, the inexorable logic of the checkpoint tragedy will repeat itself unless LLW technology and procedures are adopted.

In a desirable future, imagine a van approaching a checkpoint, which has been carefully laid out with LLW tactics in mind: a long approach with clear sight lines and pre-positioned equipment. Two soldiers are armed with LLW, and two are ready with lethal weapons in reserve. The driver misses the signal to stop. Instead of a warning shot, a few flash bang grenades explode in the road in front of the van. Assume the van continues to advance (it might stop). Instead of metal bullets to the engine, a barrage of rubber bullets smashes the front of the van, breaking the windshield without injuring anyone inside severely. The van continues to advance (it might stop). At this point the use of deadly force is arguably justified, but a spike mat rolls out in front of the van from the side of the road, triggered remotely. The tires are punctured and the van rolls to a stop a safe distance away. A panicked mother and women and children are hustled from the car, wailing and screaming: they suffer severe emotional trauma, but not injury and death.

Arguments against such elaborate devices and procedures abound. "Soldiers need to carry lethal firepower into battle, not rubber bullets and flash bangs. War is hell, and civilians get caught in the crossfire: it is deeply

> "The arguments against the development and use of at least some LLW ring exceedingly hollow, given the tragedies of civilian casualties in Operation Iraqi Freedom."

regrettable but sometimes unavoidable." Such objections do not reflect the strategic impact of modern televised warfare, where every such event will be broadcast worldwide by embedded media, if not as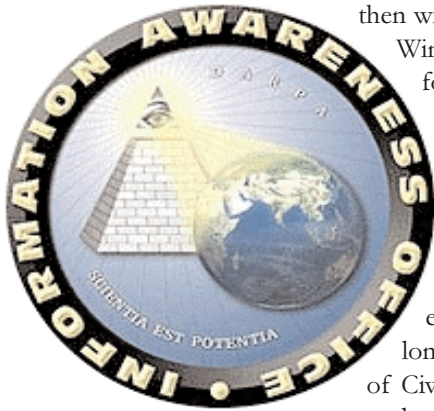 it happens, then within minutes. Winning the war for hearts and minds will be as important as wars for territorial control if we are indeed engaged in a long-term "Clash of Civilizations." A measured application of humane LLW technology on the battlefield of the future must be preferred to a repeat of the Najaf checkpoint tragedy. It is certain that lethal weapons will be used in combat and at checkpoints in places like the West Bank. I have no doubt that replacing some lethal weapons by less-lethal weapons can spare civilians and even reluctant combatants from tragic death. My sincere hope is that accelerated deployment of standard-issue LLW technology becomes a priority for military. ■

# Orwell Meets Kafka?

*Tom Karas,*
*thkaras@sandia.gov*

*I*n a logo now removed from its website, the Defense Advanced Projects Research Agency (DARPA) Information Awareness Office (*www.darpa.mil/iao*) sported the motto, *Scientia est Potentia*—Knowledge is Power.

The question for many external critics has been, who gets the knowledge and who has the power? This Office has been sponsoring a research program that includes a project looking ultimately to a "Total Information Awareness" (TIA) system (*www.darpa. mil/iao/iaotia.pdf*) that would allow intelligence analysts to "mine" data from both commercial and governmental sources to try to detect and track potential terrorists. This program has evoked considerable public controversy, and on February 11, 2003, House and Senate conferees agreed to slow it down—prohibiting, for now, its application to U.S. citizens and conditioning further research on a detailed report to Congress about its impact on privacy and civil liberties.

## Why the Fuss?

Considering the demonstrated threat of terrorism to American life and property, there certainly is a strong case for applying every possible tool to finding and stopping terrorists before they can strike. At the same time, it can be argued that if we surrender our free and democratic way of life in the name of stopping terrorism, the terrorists will have won. Does the prospect of mining our "personal" data in the hunt for terrorists pose this threat? How do we strike the right balance between our security and our rights to privacy and liberty?

Particularly since the arrival of the computer age, (and well before 9/11/2001) government agencies (state, local, and federal) and private companies (*www.choicepoint. com*) have been gathering and storing increasingly detailed and widely scoped information about us and how we conduct our lives. One legal scholar, Daniel Solove, Assoc. Prof. of Law, Seton Hall Univ., has argued that the U.S. has failed to adopt a coherent body of law and regulation for information privacy that could preserve an appropriate balance of power between individuals on the one hand and governments and corporations on the other. He also argued—at least before 9/11—that many people considered this problem in the perspective of the wrong metaphor: that of George Orwell's, *1984,* rather than Franz Kafka's, *The Trial.* That is, people thought the problem was that of "Big Brother" keeping them under constant, oppressive surveillance. Solove said that, instead, the emerging problem is that of faceless bureaucracies making arbitrary decisions about our lives, based on information about us that might or might not be true and used in ways over which we had no control. But, in the post-9/11 world, is it possible that we could see a blending of the Orwellian and Kafkaesque dystopias?

## A Catalog of Calamities

A slide from the TIA project outlines the many kinds of information kept

about us in a host of public and private databases: financial, educational, travel, medical, veterinary, border crossing, entry to places and events, transportation, housing, purchases, government interactions, communications. The fact that government or commercial agencies may be able to assemble all this information to form a picture of our lives may be generally discomfiting, but does it have tangible consequences for our lives? Many argue that it can.

Here are some of the kinds of injustice those concerned about government aggregation of personal data worry about:

- false arrest based on "false positive" data profiling (data incorrect, pattern misinterpreted, or both);

- false listing on criminal or terrorist "watch lists," with little opportunity to correct errors;

- listing as in a "suspect" category, which is later leaked and leads to public disgrace or economic deprivation or leads to round-ups in times of emergency;

- abuses of the system by malicious or over-zealous officials, e.g.

   - harassment or blackmail to stifle free expression;

   - leaking embarrassing personal details to the press;

   - surveillance that discourages freedom of association;

   - presumptions of guilt by association with "suspicious" intelligence targets;

   - "fishing expeditions" for minor infractions that can be punished in lieu of making cases for more serious suspected crimes;

- inadequate protection of aggregated information

from unauthorized access, risking:

   - identity theft
   - harassment by stalkers
   - unfair commercial disadvantages;

- inability to see and correct false information that might be used in the above ways.

## The Larger Context of Liberty

Plans to conduct data mining in search of terrorists are taking place not in isolation, but in an environment in which Constitutional protections are being relaxed in the interests of national security. For example, the government asserts the right to declare U.S. citizens to be "enemy combatants," subject to indefinite detainment without a warrant, a right to a lawyer or a trial. Orwell might meet Kafka when an anonymous law enforcement official judges a data-mined pattern to present enough suspicion



**Total Information Awareness (TIA) System**

Detect → Classify → ID → Track → Understand → Preempt
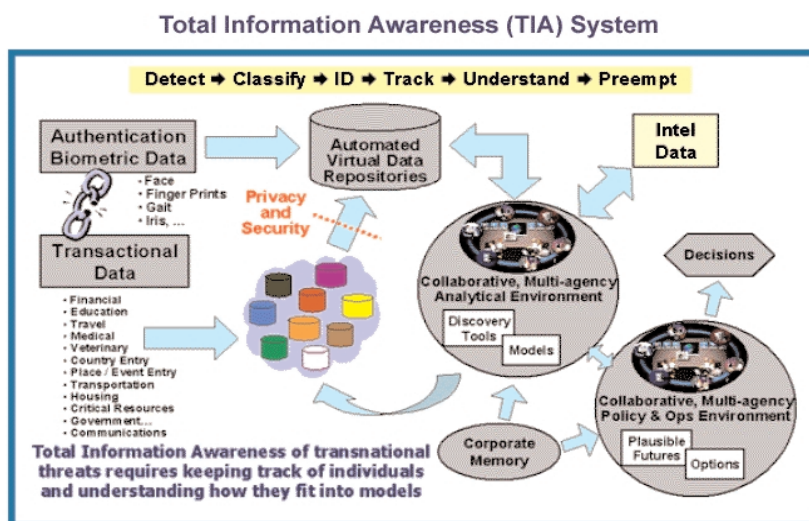
Source: DARPA's Total Information Awareness Program Homepage, http://www.darpa.mil/iao/TIASystems.htm

(Note: the above illustration is no longer posted at the website cited)

of "combatant" status that an actually innocent person is arrested and disappears into the system.

### Technology Solutions?

How well our rights to privacy and our civil liberties survive the new applications of information technology to the hunt for terrorists will depend not just on the technology, but also on the laws, regulations, rules, and practices that govern their use. Thus, there is no purely technical fix to the risks described in this article. However, if our government establishes a meaningful set of regulating principles, then it may be that technologies can be devised to help make sure those principles are adhered to in practice. We now turn to that possibility.

During an ACG "brainstorm" last month on "data mining" for terrorist detection, a couple of participants suggested that the best argument against such a program was that it is highly unlikely to work. However, executing such a program would hardly be the first time that a government security agency chose to apply a technology *(www.nap.edu/ catalog/10420.html)* that has only a slim chance of serving its security purposes while having a better chance of harming innocent persons. The question then becomes, if the technology is coming willy-nilly, are there at least methods to reduce the risks?

### Decreasing False Suspicions

Counterterror intelligence analysts might use data mining techniques in two ways. First, they might begin with suspicions about some person and then search multiple data sources to build a dossier on that individual. This is the more traditional investigative approach. Ultimately, the best protection against false suspicion remains the wisdom of the investigators; theoretically, giving them more information to confirm or disconfirm their suspicions will reduce the number of false accusations. On the other hand, if apparently incriminating information in the databases is itself untrue, it might seem to confirm a previously doubtful suspicion.

The second data mining approach is an automated search of data encompassing a very large population for patterns of transactions and social network connections that might indicate terrorist-related activity. This approach at least has the virtue that the vast majority of "dossiers" assembled about individuals are only virtual (not permanently stored) and are processed by machines, not humans who might abuse the information. Nevertheless, once the machines flag suspicious patterns, individuals are singled out as suspects.

Individuals coming under suspicion by this route then get further investigated or placed under surveillance. The first tool for preventing false suspicions in this approach is a set of powerful algorithms that point only to the most probable cases of wrongdoing. Whether such algorithms can actually be developed, of course, remains to be seen. The second way to minimize false suspicions is, again, to assure the accuracy of the data.

Two kinds of measures might, to some extent, ease the problems of inaccurate data. One is to "label" the various pieces of data so as to identify and score the probable reliability of the source. Thus, at least in some cases, the investigators would be cued to be suspicious about the data itself, rather than assuming all pieces of the assembled picture to be equally valid. A second kind of protection might come if individuals had access to at least some of the information about them in the databases being mined, plus an easy and effective set of procedures for correcting misinformation. (For more on this problem, see below.)

### Preventing Official Abuses

In some cases, false accusations may arise not just from poor information or analysis, but from over-zealousness—erring on the side of suspicion. As bad, or worse, malicious officials might abuse their access to people's data by using it to persecute them in various ways. To guard against such possibilities, we have: guidelines, rules, regulations and laws to govern official behavior; administrative oversight mechanisms; and

judicial and legislative oversight of executive operations. All these involve accountability of investigators to other parties—such as supervisors, inspectors general, review boards, external monitoring agencies, judges, and lawmakers.

To some extent, technology can be applied that would help enforce accountability. Examples follow.

### ACCESS LIMITATION

*Limitations on Purpose.* One suggested rule is that data mining such as that envisaged in the Total Information Awareness program should be limited to counter-terrorism—and that other law enforce-ment investigations would be out of bounds. This might limit access to the data to officials directly involved in counter-terrorism, rather than exposing the data to hundreds of thousands of law enforcement officials and raising the chances of abuse. Strong encryption and access control technologies would enforce this rule, allowing access only on some certified need-to-know basis.

*Selective Revelation.* A data mining system might also gradate levels of detail according to the level of analysis. For example, the actual identity of suspect "x" might be concealed from the analyst until some threshold of suspicious patterning is reached. In addition, just as data might be labeled according to its reliability, it might also be labeled according to the privacy rules that should govern it. At the

point where levels of privacy protection need to be crossed, the analyst would have to seek permission, with explanation, from some monitoring party to proceed to greater levels of detail—or might have to pass the suspect pattern on to a smaller, more privileged group of analysts.

### AUDIT TRAILS

It may be possible to equip the system with a thorough, tamper-resistant and tamper-evident audit trail that shows who has accessed what information. Then leaks or other malicious uses of the information could more easily be tracked down and abusers punished. Such a system might itself require automated data mining techniques to reveal patterns of abuse and bring them to the attention of monitors.



**Keeping the Crooks out**

The counterterrorist data mining system would need to prevent unauthorized users from either utilizing its processes for criminal purposes or from gaining access to the data it had aggregated on individuals. The main tool for preventing unauthorized access is information security—data encryption and user identi-fication and authentication.

It may be argued that the various commercial or local government databases that the government data mining system would draw on will not all have particularly sound security programs. On the one hand, this problem would exist whether the government were utilizing the data or not. On the other hand, one can imagine malicious use of the very fact that the government had been collecting information on one individual or another. In that case, abuse would arise out of the federal government activity, but by a means (leakage from non-federal databases) over which the government had no control.

**Minimizing False Information**

Technically, it might be possible to give people access to the personal information being kept about them in commercial, and at least some governmental, databases. They might also be given the opportunity to correct directly information that has supposedly been self-reported and to challenge the accuracy of information about them reported to others. One now has such opportunities under the Fair Credit Reporting Act *(www.ftc.gov/os/statutes/fcra.htm #611).* The practicality of extending these measures to all the other kinds of databases containing personal informa-tion remains to be seen. And intelligence and law enforcement agencies will want to be excluded on the grounds that "bad guys" could find out what was known about themselves.

> "It may be possible to equip the system with a thorough, tamper-resistant and tamper-evident audit trail that shows who has accessed what information."

Some suggest that people could be notified when the government has obtained their personal information and what has been done with it. This seems technically feasible, but, again, the intelligence and law enforcement agencies would resist. Not only would criminals learn that they were under surveillance, if they knew what kinds of information were being collected (even if it were not their own information), they would have insight into intelligence methods and could adapt their behavior accordingly. Some delay (a year? two years?) between collection and notification might alleviate the first problem in some cases but not the second.

### Other Ideas?

The list of technological "fixes" offered here is not necessarily exhaustive. Do you have other suggestions? Please pass them along to us via email.

### The Bottom Line

The various technologies described above may well help a government concerned about privacy and civil liberties to protect such individual rights while enhancing its ability to hunt down terrorists. But there is bound to be a tension between the goals of liberty and security. If intelligence and law enforcement officials, judges, and lawmakers are convinced that the public is ready to curtail liberties in exchange for additional security against terrorists, then they will not see much need to invest in the

technologies that might limit governmental freedom of action.

### Some Additional Reading Recommendations

ACLU, *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society,* Jan. 15, 2003 (*www.aclu.org/ Privacy/Privacy.cfm?ID=11573 &c=39*)

Matthew Brzezinski, *Fortress America*, New York Times Magazine, Feb 23, 2003. (*www.nytimes.com/2003/02/23/ magazine/23FORTRESS.html?e x=10469933159&ei=1&en=4 101225b58320d45*)

DARPA-sponsored study, *Security with Privacy,* December 2, 2003. (*www.darpa.mil/iao/ secpriv.pdf*)

*Human Rights,* (vol. 29, no. 1 (Winter 2002) (*www.abanet. org/irr/hr/winter02.html*)

Markle Foundation Task Force, *Protecting America's Freedom in the Information Age* (October 2002) (*www.markletaskforce.org*)

Daniel J. Solove, *Access and Aggregation: Privacy, Public Records, and the Constitution* 86 Minnesota Law Review 1137 (2002) (*http://law.shu.edu/ faculty/fulltime_faculty/soloveda/ access_aggregation.pdf*)

Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy* 53 Stanford Law Review 1393 (2001) (*http://law.shu.edu/ faculty/fulltime_faculty/soloveda/ kafka_orwell_privacy.pdf*)

U.S. ACM Public Policy Committee letter to Senate Armed Services Committee (*www.acm.org/usacm/Letters/tia _final.html*). ∎

# Wicked Problems Part A: The Definition

JOHN WHITLEY, JBWHITL@SANDIA.GOV

*A* 1973 paper introduced the concept of "Wicked Problems"—arguing that social policy is not amenable to solutions using "scientific" processes and analysis. The authors, Horst Rittel and Melvin Webber, (professors of design and of city planning), argued that in social planning

> *"there is no such thing as 'undisputable public good;' there is no objective definition of equity; policies that respond to social problems cannot be meaningfully correct or false; ...Even worse, there are no 'solutions' in the sense of definitive and objective answers."*

They used the term "wicked" not in the sense of evil or ethically deplorable, but in the sense of being "vicious" or "tricky" or even "malignant." A wicked problem is ill-defined, complex and relies on "elusive political judgment for resolution." In contrast, a "tame" problem (which may still be complex) is "…definable and separable and may have solutions that are findable." Problems in the natural sciences and in engineering are often tame. For a tame problem, the mission is clear—and so is whether the problem is solved or not. In the past, Sandia has concentrated on

---

**"They used the term "wicked" not in the sense of evil or ethically deplorable, but in the sense of being 'vicious' or 'tricky' or even 'malignant.'"**

tame (even if challenging) problems, but now it is starting to tackle more wicked problems—such as the war on terrorism. In this article, I will summarize Rittel and Webber. Next month I'll discuss tools and techniques that can be used to tackle wicked problems.

**The Characteristics of Wicked Problems**

Rittel and Webber define ten distinguishing properties of wicked problems.

1. NO DEFINITIVE FORMULATION. For a given tame problem "…an exhaustive formulation can be stated containing all the information the problem-solver needs for under-standing and solving the problem." In contrast, "The formulation of a wicked problem is the problem…every specifica-tion of the problem is the specification of the direction in which a treatment is considered." This is probably the most difficult concept to accept for those of us accustomed to tackling problems with a systems approach. The systems analyst may say, "just give me your requirements."

But how do we formulate the problem of, say, terrorism? Exactly what is the formulation of the problem? Is it a lack of physical safety? An excess of fear? A lack of communication and understanding between cultures? Insufficient surveillance and intelligence? Loss of our freedom? Failed states that

harbor terrorists? Formulating the problem includes assumptions about the solutions. A wicked problem must be approached realizing that "one cannot understand the problem without knowing about its context; one cannot meaningfully search for information without the orientation of a solution concept; one cannot first understand, then solve."

2. NO STOPPING RULE. Since wicked problems have no definitive formulation, there is no end to the casual chains that link all the interacting open systems. Work on wicked problems is not terminated for reasons inherent to the "logic" of the problem, but for external considerations: one runs out of time, or money, or patience. One ends work on the problem with "that's good enough," or "I like this solution."

3. SOLUTIONS TO WICKED PROBLEMS ARE NOT TRUE-OR-FALSE, BUT GOOD-OR-BAD. There are conventional criteria for judging the success of a solution to a tame problem. For example, the evaluation of whether a bridge design meets the specifications could be done by any qualified engineer and the results would be normally unambiguous. But when it comes to wicked problems, many parties are equally equipped, interested or entitled to judge the solutions; and all are equally qualified to set the criteria for determining correctness. We can see this problem occurring in our

war on terrorism, with the "goodness" of proposed solutions dependent on individual or group value-sets and ideological predilections. "Good or bad," "better or worse," "satisfying," or "good enough" seem to be the best we can hope for.

4. THERE IS NO IMMEDIATE AND NO ULTIMATE TEST OF A SOLUTION TO A WICKED PROBLEM. Any attempt at a solution to a wicked problem will send waves of repercussions through the system. There is no way of judging the total effect of the solution until all these waves have completely run out, and we really don't have ways of even tracing all the waves through all the affected lives.



5. EVERY SOLUTION TO A WICKED PROBLEM IS A "ONE-SHOT OPERATION;" BECAUSE THERE IS NO OPPORTUNITY TO LEARN BY TRIAL-AND-ERROR, EVERY ATTEMPT COUNTS SIGNIFICANTLY. In the realm of physical engineering, one can usually design a develop/ test/prototype cycle that lets one try out various design approaches without penalty. In the realm of social engineering, most actions are effectively irreversible and the half-lives of consequences are long. Hence, every trial counts. One cannot give up civil liberties in the pursuit of safety with the plan to simply reverse the decision if it doesn't work out.

6. WICKED PROBLEMS DO NOT HAVE AN ENUMERABLE (OR AN

EXHAUSTIVELY DESCRIBABLE) SET OF POTENTIAL SOLUTIONS, NOR IS THERE A WELL-DESCRIBED SET OF PERMISSIBLE OPERATIONS THAT MAY BE INCORPORATED INTO THE PLAN. Unlike physics or chemistry or engineering problems, wicked problems are only amenable to plans of action that depend on judgment, and on enough trust and credibility between planner and clientele to lead to agreement to act.

7. EVERY WICKED PROBLEM IS ESSENTIALLY UNIQUE. Wicked problems often have distinguishing properties of overriding importance that make it difficult to group them into general classes. For example, problems and solutions relating to border crossings with Mexico will probably differ in essential ways from those relating to border crossings with Canada. A successful program to counter terrorism in Indonesia will differ substantially from one for Pakistan. As the authors state, "part of the art of dealing with wicked problems is the art of not knowing too early which type of solution to apply."

8. EVERY WICKED PROBLEM CAN BE CONSIDERED TO BE A SYMPTOM OF ANOTHER PROBLEM. A wicked problem comprises interlocking issues and constraints that change over time and are em-bedded in a dynamic social context. There is no "natural" level of analysis

for a wicked problem. At too high a level, the problem definition is too general to act on; at too low a level, one can only address symptoms. Increasing security at airports frustrates passengers and adds cost— which decreases travel and burdens airlines, which requires higher ticket prices, which decreases air travel more (or requires government bailouts), which makes people drive more, which increases congestion, and on and on.

9. THE EXISTENCE OF A DISCREPANCY REPRESENTING A WICKED PROBLEM CAN BE EXPLAINED IN NUMEROUS WAYS. THE CHOICE OF EXPLANATION DETERMINES THE NATURE OF THE PROBLEM'S RESOLUTION. There are many stakeholders who will have various and changing ideas about what might be a problem, what might be causing it, and how to resolve it. For example, if one wishes to reduce crime, you might increase the number of police officers. If, over the next two years, there is an increase in arrests, but also an increase in crime, but at a lower rate than was predicted, then has the "solution" been effective? With wicked problems, there are as many debates about the meanings of observed effects as there are about solutions. People choose those explanations that are most plausible to them.

10. THE PLANNER HAS NO RIGHT TO BE WRONG. As scientists, we can forward hypotheses for testing with little impact outside our own world (perhaps just our reputation and maybe some misdirected funding). Knowledge, even negative knowledge, is valued. So long as scientists follow the rules of the game, no one is "blamed" for postulating hypotheses that are later refuted. In the world of wicked problems, however, decisions have real consequences on real people. Mistakes hurt people; money wasted on failed solutions depletes resources. The aim of solutions to wicked problems is not to discover some "truth" but to right some wrong or to better the world. Every attempt matters.

Rittel and Webber observe that in modern pluralistic societies there are "…no value-free, true-false answers to any of the wicked problems governments must deal with." Social planners have "neither a theory that can locate societal goodness, nor one that might dispel wickedness, nor one that might resolve the problems of equity that rising pluralism is provoking." Part B of this series will discuss this discouraging state of affairs and some methods for dealing with it. ■